

FMC에서 관리하는 FTD의 관리 인터페이스 IP 주소 변경

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Secure Firewall Management Center에서 관리되는 방화벽 위협 방어 디바이스의 관리 IP를 변경하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Secure Firewall Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.2.5(1)를 실행하는 Secure Firewall Management Center Virtual
- 버전 7.2.4를 실행하는 Cisco Secure Firewall Threat Defense Virtual

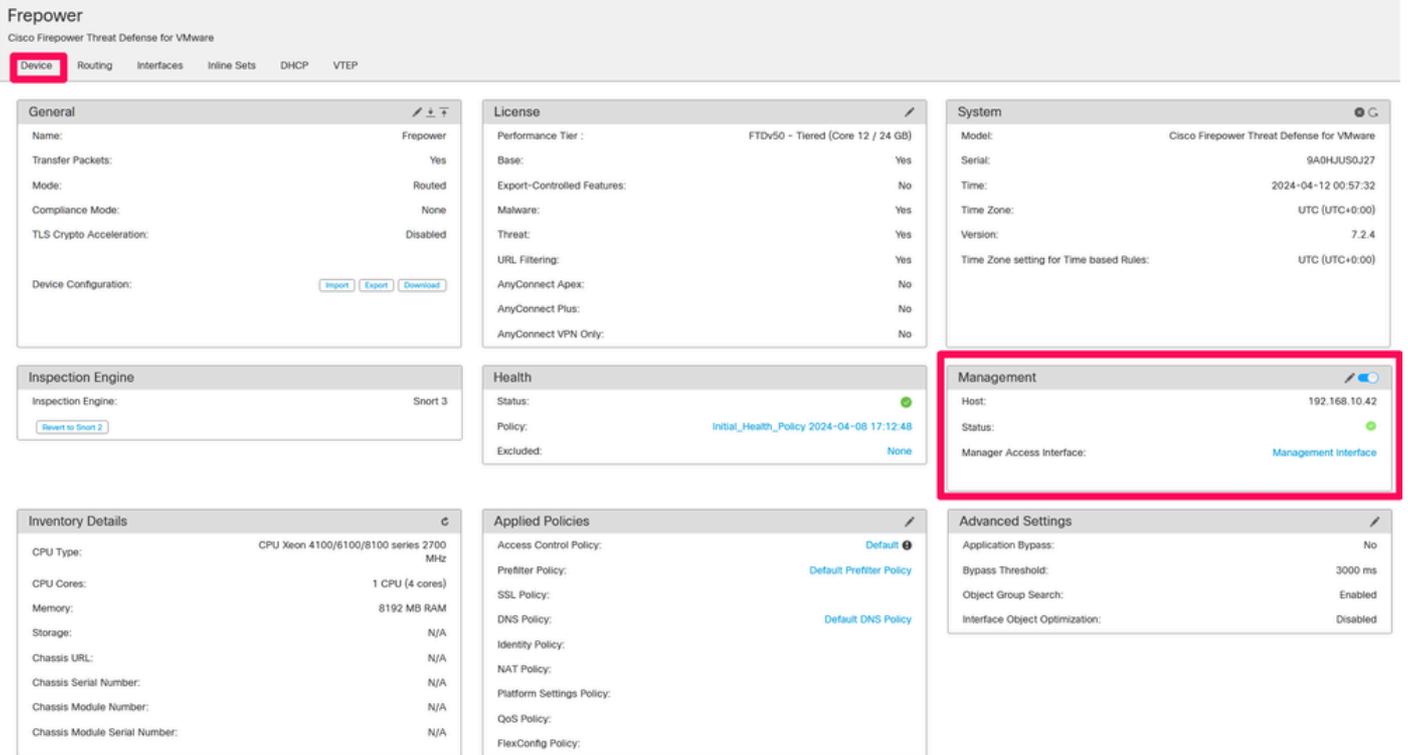
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

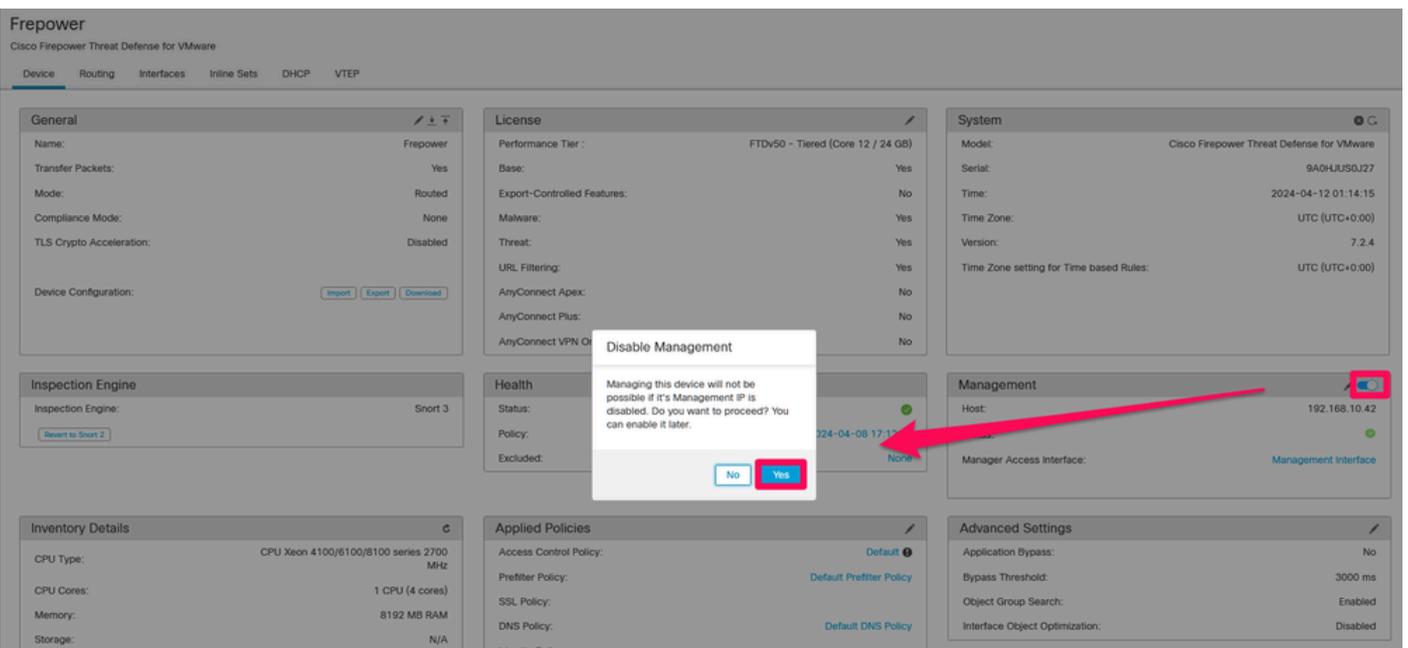
설정

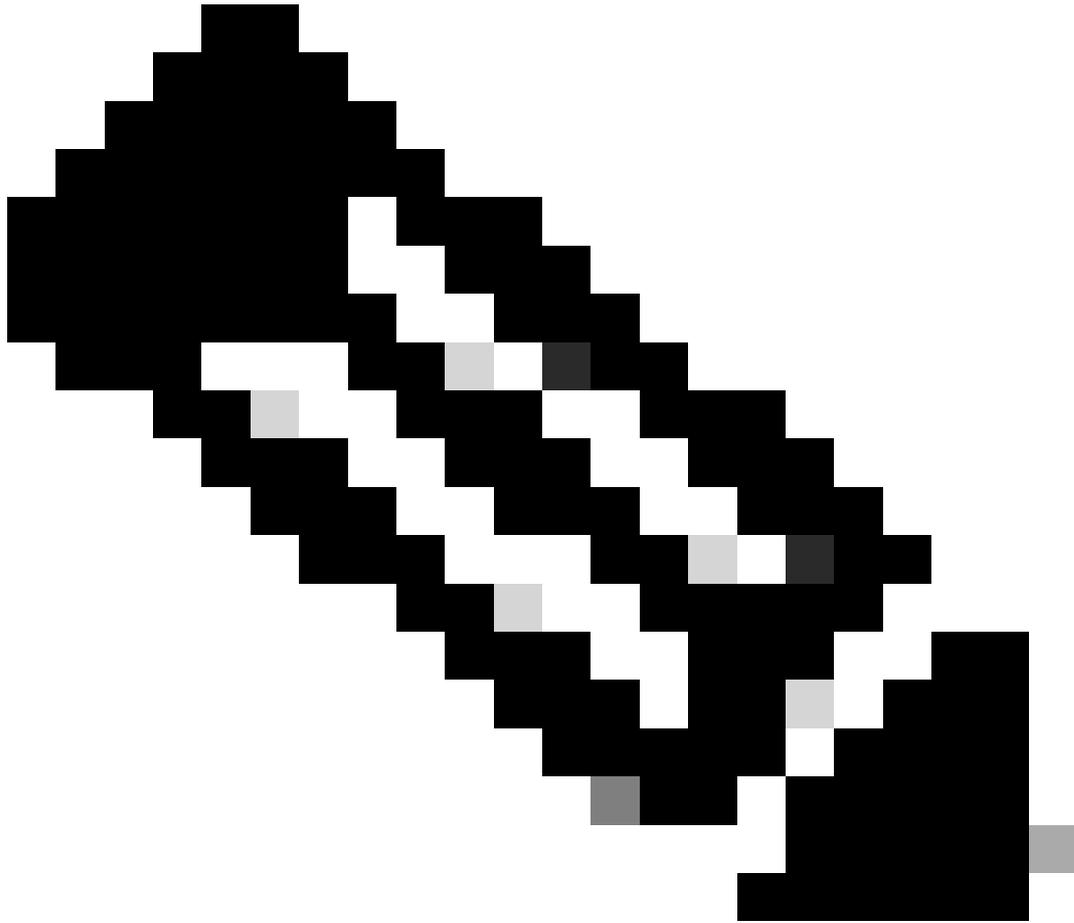
1단계. FMC GUI로 이동하고 Device(디바이스) > Device Management(디바이스 관리)로 이동합니다.

2단계. Device(디바이스)를 선택하고 Management(관리) 섹션을 찾습니다.



3단계. 슬라이더를 클릭하여 Management(관리)를 끄고 Yes(예)를 선택하여 작업을 확인합니다.

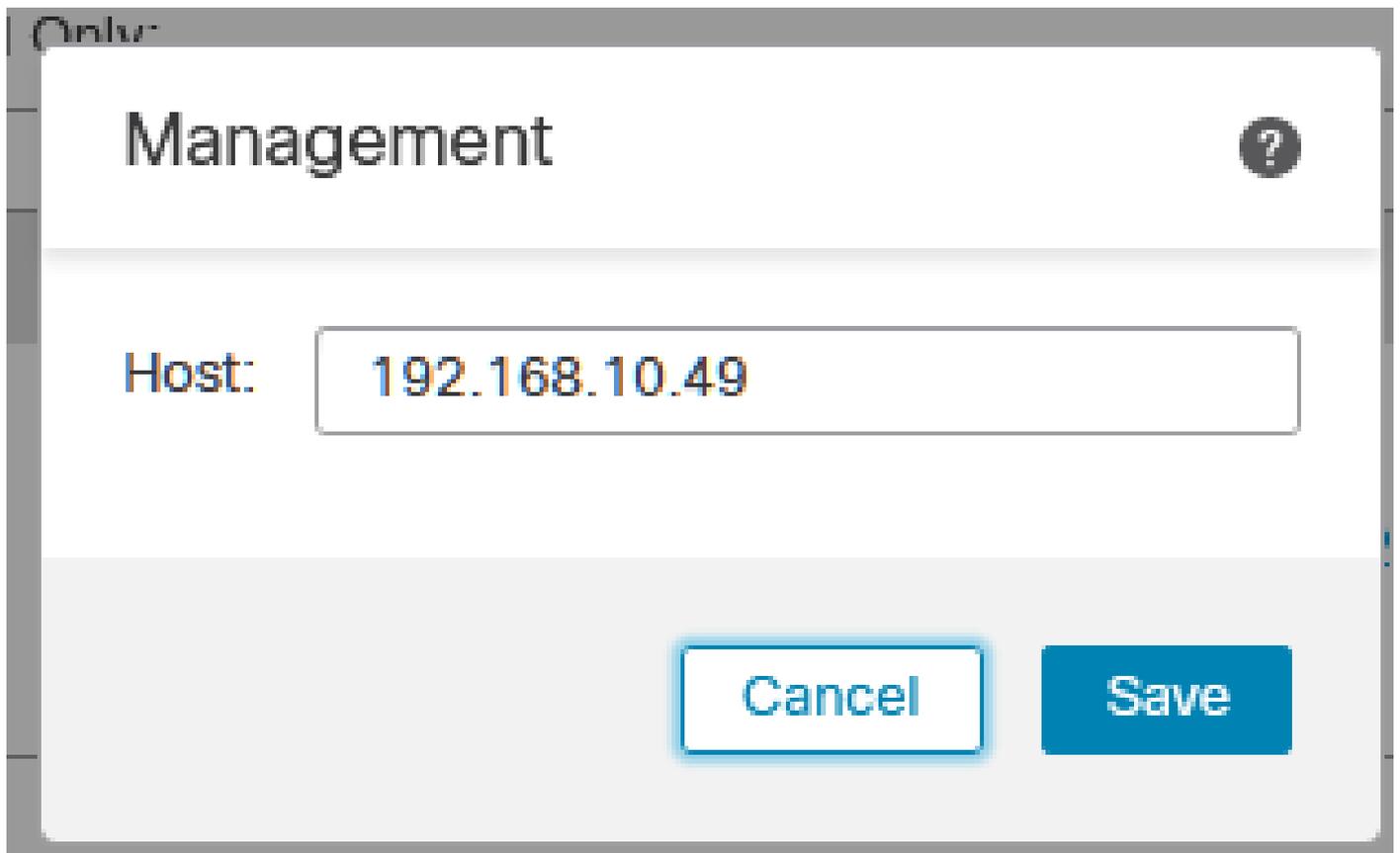




참고: Management를 해제하면 Management Center와 디바이스 간의 연결이 중단되지만 디바이스는 Management Center 내에 유지됩니다.

4단계. Management(관리)가 비활성화된 상태에서 Edit(수정)를 선택하여 관리 연결을 수정합니다.

5단계. Management(관리) 대화 상자에서 remote Host address(원격 호스트 주소) 필드의 IP 주소를 변경한 다음 Save(저장)를 선택합니다.



6단계. FTD 콘솔에 연결하여 관리 IP 주소를 수정합니다.



경고: 관리 IP 주소를 변경하면 관리 IP 주소를 통해 세션이 설정된 경우 디바이스에 대한 SSH 연결이 손실될 수 있습니다. 따라서 Cisco에서 제안하는 대로 콘솔 액세스를 통해 이 변경을 수행하는 것이 좋습니다.

7단계. Cli 모드에서 다음 명령을 사용하여 관리 IP 주소를 수정합니다.

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```



참고: 이 컨피그레이션은 기본적으로 관리 인터페이스에 적용됩니다.

8단계. FMC GUI로 돌아가 Slider(슬라이더)를 On(켜기) 위치로 전환하여 Management(관리)를 다시 활성화합니다.



9단계. 관리 연결을 다시 설정하는 데 다소 시간이 걸릴 수 있습니다. 이 이미지에 표시된 대로 재연결이 성공했음을 알 수 있습니다.

Management 	
Host:	192.168.10.49
Status:	
Manager Access Interface:	Management Interface

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FTD CLI를 통해 관리 연결을 확인할 수 있습니다. 이 명령은 다음 명령을 실행하는 Cli 모드에서 CLI에 연결하면 됩니다.

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
```

```
-----OUTPUT OMITTED-----
```

```
*****
```

```
**RPC STATUS**192.168.10.40*****  
'last_changed' => 'Fri Apr 12 01:09:19 2024',  
'active' => 1,  
'ipv6' => 'IPv6 is not configured for management',  
'uuid_gw' => '',  
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',  
'name' => '192.168.10.40',  
'ip' => '192.168.10.40'
```

```
Check routes:
```

```
No peers to check
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

- FTD CLI에서 관리 연결 상태를 확인하려면 `show sftunnel status brief` 명령을 실행합니다. 피어 채널에 대한 세부 정보에 연결되어 있지 않고 하트비트 정보가 누락된 경우 표시되는 연결 중단 출력을 확인합니다.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40
```

```
Registration: Completed.
```

```
Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC
```

Last disconnect time : Fri Apr 19 21:14:23 2024 UTC

Last disconnect reason : Both control and event channel connections with peer went down

FTD CLI의 `sftunnel-status-brief` 명령이 정보 및 하트비트 데이터에 연결된 피어 채널을 포함하는 출력을 생성하면 디바이스 간의 정상 연결이 확인됩니다.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40
```

```
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'
```

```
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'
```

```
Registration: Completed.
```

```
IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC
```

```
Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC
```

```
Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC
```

```
Last disconnect time : Fri Apr 19 21:12:57 2024 UTC
```

```
Last disconnect reason : Process shutdown due to stop request from PM
```

- 네트워크 연결을 확인하려면 관리 인터페이스에서 관리 센터를 ping하고 FTD CLI에서 `ping system fmc_ip`를 입력합니다.

관련 정보

- [장치 관리 기본 사항](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.